UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The three (3) digital devices presently located at the U.S. Secret Service Seattle Field Office Evidence Room

Case No. MJ14-431

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A1, which is incorporated herein by reference

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B1, attached hereto and incorporated herein

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §2251(a)	Production of Child Pornography
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. §2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent John Wurster, attached hereto and incorporated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA JOHN C. WURSTER, USSS
Printed name and title

Sworn to before me and signed in my presence.

Date: 29 October 2014

Judge's signature

City and state: SEATTLE, WASHINGTON

JAMES P. DONOHUE, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT OF BRYAN MOLNAR

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, John Wurster, a Special Agent with the United States Secret Service, Seattle, Washington, having been duly sworn, state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

1. I am a Special Agent (SA) with the United States Secret Service (Secret Service) and have been so since June 21, 1999. I am currently assigned to the Seattle Field Office. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of Title 18, United States Code, Sections 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia, and the United States Secret Service, Special Agent Training Program located in Beltsville, Maryland. Prior to my employment with the Secret Service, I served in the United States Army as a Counterintelligence Special Agent. I have a Bachelor of Science Degree from Brenau University. In the course of my law enforcement career, I have investigated crimes ranging from the production and passing of counterfeit currency, identity theft, access device fraud, bank fraud and threats made against the President and Vice President of the United States. As part of my training with the Secret Service, I have received instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud and identity theft. I have also completed specialized training in the investigation of electronic crimes involving the use of computers and other electronic devices. I have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of previous search warrants, which involved child exploitation and/or child pornography offenses, and the search and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

seizure of computers, related peripherals, and computer media equipment. I am a member of the Seattle Internet Crimes Against Children Task Force, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. I make this Affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search three cellphones currently being held at in the U.S. Secret Service Evidence Vault, more fully described in Attachment A1 to this Affidavit, fully incorporated herein by reference ("JOHNSON's PHONES"), for the items described in Attachment B1 to this Affidavit, fully incorporated herein by reference; all for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (Production of Child Pornography/Sexual Exploitation of Children), 2252(a)(2) (Receipt or Distribution of Child Pornography) and 2252(a)(4)(B) (Possession of Child Pornography).

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of cooperating witnesses; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the applications for the search warrants, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251 (Production of Child Pornography/Sexual Exploitation of Children), 2252(a)(2) (Receipt or Distribution of Child Pornography) and 2252(a)(4)(B) (Possession of Child Pornography), will be found on JOHNSON's PHONES.

/////

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF INVESTIGATION

5. On or about June 12, 2014 and June 26, 2014, Microsoft Skydrive discovered one of their subscribers had uploaded ten files of suspected child pornography to the Internet on June 06, 2014 between 1406 and 1458 hours UTC. Microsoft Skydrive subsequently made two reports to the National Center for Missing & Exploited Children (NCMEC), who documented the complaint(s) in CyberTips #2520605 and #2507507. These complaints were sent to the Seattle Internet Crimes Against Children Task Force (ICAC) and subsequently referred to the Auburn Police Department.

6. Identifying information provided to NCMEC, by Microsoft Skydrive, included the IP address reportedly used to facilitate the upload of the images as 50.135.62.177 by the email address of sdjdogg@gmail.com.

7. Detectives conducted a WHOIS lookup of IP address 50.135.62.177 and found it to correspond to Comcast. Additionally, Gmail email addresses are known to be issued and controlled by Google.

8. Auburn Police Detectives Nix and Faini reviewed ten images associated with CyberTips associated on both days and observed and reported the following descriptions:

9. The file titled, 20140609_075449_Android 11.jpg, per Skydrive, is an image file which depicts a prepubescent female child victim approximately ten (10) to fourteen (14) years of age (based on body development and physical characteristics). The child victim is seen kneeling down next to a chair. Her eyes are closed and her mouth is open where she is performing fellatio on what appears to be a juvenile male child victim, approximately twelve (12) to fifteen (15) years of age (based on vellus hair present but lack of body development). This juvenile male is sitting in a chair with his eyes closed and is not wearing any clothing. Standing to the left of the male and female child is a shirtless adult female with long brown hair. This adult female is holding the juvenile male's erect penis with one hand while the other head appears to be guiding the female

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

child's head. Per information from Microsoft Skydrive, this image was posted using IP 50.135.62.177 on June 09, 2014 at 14:57:11 UTC.

10. The file titled, 20140609_075450_Android 8.jpg, per Skydrive is an image file that depicts a white prepubescent female child victim approximately seven (7) to twelve (12) years old lying down. The face of the child cannot be seen because it is out of the range of the picture. This female child's legs are spread exposing her vagina to the camera as the primary focus of the picture. She is also using her hands to spread apart her vagina. An adult male's erect penis is inserted in the female child's anus. The child victim has no breast or hip development, and does not have any pubic hair.

11. The file titled, 20140609_075449_Android 5.jpg, per Skydrive, is an image file that depicts a white a prepubescent child victim that is approximately five (5) to eight (8) years of age (based on lack of body development). The child has long black hair and she is not wearing any clothing except for a pair of dark colored boots. The child's eyes are open and she appears to be smiling. The child is sitting down on a wooden floor with her legs spread apart exposing her vagina. A white adult female with long dark hair, where half of it is in a ponytail, is lying on her stomach on the floor with her face in between the female child's legs, near the child's exposed vagina as if she were about to perform oral sex on the child victim.

12. I also reviewed these and the other images and further describe image 20140609_075449_Android12.jpg depicts a prepubescent female child victim that appears to be approximately 5-8 years of age. The child victim has no hip, breast or muscle development and no pubic hair. The child victim is fully naked in the picture and is masturbating her vagina with her right hand and is performing simulated fellatio on what appears to be a sex toy held in her left hand.

13. Based on the above information, Det. Nix believed that information regarding the identity of suspect(s) responsible for engaging in activities in violation of RCW 9.68A.070 Possession of Depictions of Minors Engaged in Sexually Explicit Conduct would be found in the account records of Comcast Cable, Microsoft Live

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Skydrive and Google. Detective Nix obtained King County Superior Court Search Warrants for Comcast IP address 50.135.62.177, Microsoft Live Skydrive, and Google email address sdjdogg@gmail.com

14. Open source internet searches were conducted on the email address sdjdogg@gmail.com and a response for SDJ Music Xray was located. This link showed a promotional webpage for an artist by the handle of SDJ (SHAWN DAVID JOHNSON). Above artist information on the page was another link that went to a "license page." This page displayed the email address sdjdogg@gmail.com.

15. Another open source internet search was run on the name "SDJ" and a website called "Shoutbox" was located bearing the same SDJ logo as was found on SDJ Music Xray. Located on the site was a section titles "About this album" stating, "SDJ was born Shawn D. Johnson." It went on to describe SHAWN DAVID JOHNSON growing up in Tacoma and being married and a father of two children.

16. SDJ was searched on Twitter and Facebook and pictures of SHAWN DAVID JOHNSON were obtained. A Twitter tweet from SHAWN DAVID JOHNSON was located stating, "Follow @kristinehopstad because she is number one lady." This led detectives to believe that this may be SHAWN DAVID JOHNSON's wife.

17. Police databases were searched for both SHAWN DAVID JOHNSON and KRISTINE HOPSTED. An address of 11660 SE 323rd PL, Auburn, WA was located for SHAWN DAVID JOHNSON based on a May, 2014 Police report. Washington Department of Licensing showed an address for KRISTINE HOPSTAD as 11660 SE 323rd PL, Auburn, WA.

18. On July 9, 2014, Comcast Cable responded to the search warrant with the following information:

Subscriber Name: Kristine Mayers.
Service Address: 11660 SE 323rd PL
Auburn, WA 98092
Telephone #: 206-484-2836

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Type of Service: High Speed Internet
Account Number: 84983400103376079
Start of Service: 5/1/2011
Account Status: Active
IP Assignment: Dynamically Assigned
Current IP Address: 50.135.62.177 on 7/9/2014
E-mail User Ids: kristine23hopst80
(The above user ID(s) end in @comcast.net)
Method of Payment: Statement sent to above address.

19. KRISTINE HOPSTAD was located on Facebook. On June 20, 2014, KRISTINE HOPSTAD changed her name from KRISTINE HOPSTAD MAYERS to KRISTINE JOHNSON and changed her profile picture to one of her in a wedding dress. Under the photo section a picture was found of KRISITINE JOHNSON kissing SHAWN DAVID JOHNSON while dressed in a wedding dress and tuxedo respectively.

20. On July 9, 2014, Auburn Police Special Investigations Unit officers made contact with children playing in the driveway of 11660 SE 323rd PL Auburn, WA. The children advised Auburn PD officers that SHAWN DAVID JOHNSON was their father. A vehicle was also observed in the driveway bearing Washington Registration ADR6773 which the Washington Department of Licensing Database showed to be registered to SHAWN DAVID JOHNSON.

21. On July 14, 2014 Auburn PD Det. Nix received a Google response to the search warrant. A review of other records provided by Google showed a gallery of pictures that had been uploaded by the user, SHAWN DAVID JOHNSON, and saved to his email account of sdjdogg@gmail.com. These images were pictures of SHAWN DAVID JOHNSON and his current family (family photos). Images of SHAWN DAVID JOHNSON and his family were previously located on the Internet during the open source searches. The children consisted of a young juvenile male with short brown hair, a young

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

juvenile female with glasses and long blond hair, and a prepubescent female with shoulder length curly hair.

22. During a review of this gallery of photos, law enforcement officers located several voyeuristic images of a naked, juvenile female in a bedroom. In these images, it appeared that the camera was covertly hidden in a position unknown to the victim child as she is getting dressed after taking a shower. Some of these files were reviewed and are described as follows:

23. File 1 contains three (3) images of the exact same picture; however the additional two (2) images were manipulated by altering the lighting effects, cropping the image and placing of a boarder around the image. This file that contains the three (3) images is named "hgm-2-13-10-01-11h55m37s133.jpg" and depicts a white juvenile female child victim who appears to be 10-14 years of age based on body development. The child victim is later identified as H.M. (DOB September 2000), SHAWN DAVID JOHNSON's step-daughter. H.M. is completely naked with only a dark colored towel wrapped around her hair. H.M.'s arms are up, above her shoulders, blocking a view of her face, and appear to be adjusting the towel. In the picture, a set of dresser drawers set against a light colored wall with a picture frame hung on this wall can be seen. The camera that took this photo appears to be set at a lower angle, close to the floor, because it captured the image at an upward angle. The edges of the image are not a clean, as there appears to be something blocking the upper left and corner area.

24. File 2 contains one image and is named "hgm-2013-12-04-07h40m27s212~2.jpg." This image depicts H.M. H.M.'s breasts are exposed. Her arms are raised above her shoulders and are adjusting a light colored towel on her head. A grey t-shirt has been pulled over her head and arms but just resting above her breasts. H.M. is wearing red underwear. Behind H.M., a tan colored carpet, a brown floor heater, red curtains and a white cell phone on a black object can be seen. The camera that took this image appears to be placed higher than the height of the child due to the downward angle.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

25. File 3 also contains one image named "hgm-2013-12-08-15h39m00s226~2.jpg" and depicts H.M. H.M.'s face is visible in this picture. H.M.is naked and she only has a yellow towel wrapped around her hair. She is holding a teal colored item and looking down. Hanging on the wall behind the victim is a Washington State vehicle license plate, however only the bottom half of the first numbers are visible. The camera for this picture appears to be placed back behind objects due to the fact that the left and right sides of this image is obstructed.

26. File 4, named "hgm-2013-12-08-15h37m07s180.jpg" depicts H.M. in the same scene, camera angle/obstructions, as listed in File 3; however she is completely naked and she is wrapping the yellow towel around her body. The left side of H.M.'s face is visible and her long blonde hair is visible and appears to be wet. Also, the Washington State vehicle license plate is more visible. The last letters of this vehicle plate is listed as "TTU" and although the first three bottom numbers are only half visible, they are consistent with "682" based on the shape.

27. This vehicle plate, 682-TTU, was ran through WACIC/NCIC. Results showed that this vehicle plate expired on 7-12-2012 and was registered to KRISTINE MAYERS at the address of 11660 SE 323rd PL Auburn, County of King, WA.

28. Continuing on July 14, 2014, Auburn PD Detectives obtained a King County Superior Court Search Warrant for the address of 11660 SE 323rd PL Auburn, County of King, WA. They responded to the residence and located SHAWN DAVID JOHNSON arriving home. They were able to detain SHAWN DAVID JOHNSON with no incident. Detectives observed a Samsung Galaxy phone in this vehicle that was attached to the dash by a phone holder.

29. SHAWN DAVID JOHNSON was interviewed by Detectives Nix and Faini. Post Miranda, SHAWN DAVID JOHNSON admitted to down loading depictions of children engaged in sexually explicit conduct and covertly hiding and using video recorders to obtain images in his 14 year old step-daughter's (H.M.) bedroom for sexual gratification. SHAWN DAVID JOHNSON admitted to coordinating the recording of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

video when he knew she would be in the room nude, such as her returning from taking a shower.

30. Upon questioning, SHAWN DAVID JOHNSON admitted that he has used the downloaded images and the nude images of H.M. to masturbate multiple times. SHAWN DAVID JOHNSON explained that he would capture the images of H.M. with a Droid Razor cell phone, a Samsung Galaxy S5 cell phone, a HTC First cell phone and a Belkin night vision camera. He would then use his HP laptop computer to upload these images from his cellular or electronic devises to his free Microsoft Skydrive.

31. During the interview, SHAWN DAVID JOHNSON explained in more detail how his Belkin wireless camera worked. SHAWN DAVID JOHNSON admitted he had covertly inserted the camera into the wall of H.M.'s bedroom. The camera system had two functional mode systems; a live-stream video mode and a motion activated camera mode. The live-stream video could be controlled with a cell phone application that he downloaded onto his Samsung Galaxy cell phone, which is the same cell phone that he had in his car at the time of his arrest. SHAWN DAVID JOHNSON stated he could then control when the video would start the recording, and watch it in real time as it recorded. However, the motion activated camera, which took still photos, was active all the time. When the camera sensed any motion, it would begin taking photos. Those photos would automatically be sent to SHAWN DAVID JOHNSON's Yahoo.com account, which he identified as sdjdogg@yahoo.com. SHAWN DAVID JOHNSON would then log into his Yahoo.com account and review the photos.

32. SHAWN DAVID JOHNSON also admitted during the interview that he downloaded depictions of children engaged in sexually explicit activity to computer and then uploaded them to his Skydrive account via his email account of sdjdogg@gmail.com. SHAWN DAVID JOHNSON stated not long after he uploaded the items, Microsoft shut down his account. SHAWN DAVID JOHNSON admitted he downloaded the depictions of children engaged in sexually explicit activity because of "boredom." SHAWN DAVID JOHNSON also stated it was, "taboo, risqué thing to do."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

33. SHAWN DAVID JOHNSON was asked what attracted him to women. SHAWN DAVID JOHNSON replied, "Breasts and a nice figure." When asked what attracted him to H.M. as she had more of a prepubescent figure, SHAWN DAVID JOHNSON replied, "I don't want to answer that."

34. Later in the interview SHAWN DAVID JOHNSON was asked about what his thought about when masturbating, specifically if he thought about sex with H.M. or any other child. SHAWN DAVID JOHNSON replied that he would only masturbate to the image, not on acting out any sexual intercourse with the child. SHAWN DAVID JOHNSON stated he would go to websites such as www.motherless.com and www.stickem.com to watch videos of young girls undressing. SHAWN DAVID JOHNSON stated it excited him because the young girls looked happy as they stripped to full nudity. SHAWN DAVID JOHNSON said the sites were no longer active and he assumed it was because of the child pornography.

35. SHAWN DAVID JOHNSON also explained that he would view a majority of the child pornographic images via Tumblr, which he had an active account with. Tumblr is a media network that allows users to create, post, share, and follow the digital media. SHAWN DAVID JOHNSON stated to Detective Faini that his user name for Tumblr is "sdjmusic." He denied uploading photos to Tumblr but he stated he had saved child pornographic images within his account on Tumblr that he had located from the Tumblr web site. When asked about his password SHAWN DAVID JOHNSON explained that he did not know because he is "always logged on" through is cell phone.

36. During the execution of the search warrant at SHAWN DAVID JOHNSON's residence, Detectives seized digital media and electronic devices capable of storing images and videos. On July 17, 2014, Det. Nix turned over a Nikon Coolpix camera, a JVC digital camcorder, a second camera, a HP Laptop computer and a Scan Disk seized during the execution of the search warrant on SHAWN DAVID JOHNSON's residence, to Det. Tim Luckie, Seattle Police ICAC unit for the purpose of a forensic investigation pursuant to a King County Superior Court Search warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

37. On August 26, 2014, Det. Luckie provided Det. Nix preliminary results from his forensic examination. Multiple video and image files containing images depicting minors engaged in sexually explicit activity were located. Additionally, surreptitiously made video and image files created by SHAWN DAVID JOHNSON of H.M. naked in her room were located.

38. Between September 26 and September 30, 2014, I reviewed items located by Det. Luckie and observed the following: The video file VID_20140624_014901 is an approximately 28:41 long video file depicting H.M.'s bedroom. This was confirmed by Det. Nix who also saw the video as well as H.M.'s bedroom during the execution of her search warrant. In the beginning of the video, SHAWN DAVID JOHNSON's face is seen as he turns the camera on and hides it on the floor. SHAWN DAVID JOHNSON is also seen placing a piece of gauze type cloth over the camera. It should be noted, during his interview, SHAWN DAVID JOHNSON stated to Det. Faini that he would cover the camera with cloth so H.M. would not see it.

39. At approximately 7 minutes into the video, H.M. is seen walking into the room, placing something onto the bed and walking out. At approximately 19:13 minutes into the video H.M. is seen walking into the room completely naked. H.M. stands almost directly over the camera and bends over multiple times with the focus of the camera being on her genitals and anus in a lewd and lascivious manner.

40. In going through other files I located an image file titled "Collage _2". This was a homemade collage comprised of six images H.M. The image on the far left is H.M. fully clothed with a green frog face painted on her right cheek. The center picture is H.M wearing green underwear and putting on a shirt. The focus of the photograph is H.M.'s bare breasts. The top right photograph is H.M. again putting on a shirt. Her left arm is in front of her face and her bare breasts are visible. The right photograph second from the top is H.M. drying her back while the picture is taken of her nude from the knees to the top of her head, showing her vagina and breasts. The photograph located on the right side, two from the bottom is H.M. drying her hair with her bare left breast

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

visible; however the primary focus of the camera is her bare vagina. The bottom right picture depicts H.M. naked from the bottom of her naked vagina to the top of her naked breasts.

41. I also observed image file hgm-2014-05-14-05h18m31s230.jpg. This image depicts H.M. in her room, completely naked. In this image H.M. is only visible from the waist down, with the primary focus of the camera being her naked vagina. The camera is surreptitiously placed angled down on what appears to be a shelf, hidden behind other items.

DEFINITIONS AND TECHNICAL TERMS

42. Set forth below are some definitions of technical terms, most of which are used throughout this Affidavit pertaining to the Internet and computers generally.

a. Computers and digital devices: As used in this Affidavit, the terms "computer" and "digital device," along with the terms "electronic storage media," "digital storage media," and "data storage device," refer to those items capable of storing, creating, transmitting, displaying, or encoding electronic or digital data, including computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks and tablets, smart phones and personal digital assistants, printers, scanners, and other similar items.

b. Internet Protocol (IP) Address: Typically, computers or devices on the Internet are referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address consists of four numeric sequences, separated by a period, and each numeric sequence is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each Internet Service Provider (ISP) a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is, they allocate any unused IP address at the time of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial up session. Once the session ends, the IP address is available for the next dial up customer. On the other hand, some ISPs, including some cable providers, employ static IP addressing, that is, a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

c. Hash Value: "Hashing" refers to the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data. This numerical identifier is called a "hash value." A hash value can be thought of as a "digital fingerprint" for data. If the data is changed, even very slightly (like through the addition or deletion of a comma or a period in a text file), the hash value for that data would change. Therefore, if a file such as a digital photo is a hash value match to a known file, it means that the digital photo is an exact copy of the known file.

SUBJECT'S USE OF ELECTRONIC COMMUNICATION SERVICE

43. As outlined above, SHAWN JOHNSON, using JOHNSON's PHONES, manufactured images depicting the sexual exploitation of a child and transferred those images from JOHNSON's PHONES to his computer and other phones, over the Internet.

TECHNICAL BACKGROUND

44. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

45. I know, based on my training and experience, that many cellular phones (referred to herein generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smart phone on their person; recent investigations in this District have resulted in the discovery of child pornography files on smart phones which were carried on an individual's person at the time the phones were seized.

46. As set forth above and in Attachment A1 to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above referenced crimes that might be found on JOHNSON's PHONES, in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B1 to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

a. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is collected, distributed, and produced. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these images was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership based/subscription based websites to conduct business, allowing them to remain relatively anonymous.

b. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography as described in subparagraphs (c) through (f) below.

c. Producers of child pornography can now produce both still and moving images directly from the average video or digital camera. These still and/or moving images are then uploaded from the camera to the computer, either by attaching the camera to the computer through a USB cable or similar device, or by ejecting the camera memory card from the camera and inserting it into a card reader. Once uploaded

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to the computer, the images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to those by which a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. Producers of child pornography can also use a scanner to transfer printed photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

d. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers, including ISPs, allow email service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet. Having said that, however, this application does not seek to reach any host computers. This application seeks permission only to search JOHNSON's PHONES.

e. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography, and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the distributor's/recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the distributor/recipient.

f. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage elsewhere. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

47. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years.

d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

48. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result of this information and in light of the current phase of the investigation including JOHNSON'S statements to law enforcement detailing his illegal activities, I believe that electronic evidence may be stored on JOHNSON's PHONES.

49. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachments A1 and B1 may take the form of files, documents, and other data that is user generated and found on a digital device. In other cases, these items may take the form of other types of data – including in some cases data generated automatically by the devices themselves.

50. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that there is probable cause to believe that the items set forth in Attachment B1 will be found on JOHNSON's PHONES, for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user generated files, digital devices – in particular, a computer's internal hard drive – contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information – and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. Secret Service agents in this case have specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

SEIZURE OF DIGITAL DEVICES

51. On July 14, 2014, Auburn Police Department executed a search warrant issued from King County Superior Court at SHAWN DAVID JOHNSON's residence. On July 17, 2014, the Auburn Police Department executed another search warrant issued from King County Superior Court on SHAWN DAVID JOHNSON's 1991 Dodge Dynasty vehicle. A number of digital devices, including JOHNSON's PHONES, were seized pursuant to these warrants. This warrant application seeks permission to search

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

JOHNSON'S PHONES that are currently located in the secure facility of the U.S. Secret Service Evidence Vault.

SEARCH OF JOHNSON'S PHONES

52. As set forth above, I seek permission to search JOHNSON's PHONES as more fully described in Attachment A1 to this Affidavit for the items described in Attachment B1 to this Affidavit, that is, evidence, fruits, and instrumentalities of the above-referenced crimes, in whatever form they may be found. In accordance with the information in this Affidavit, law enforcement personnel, to include the case agent, will execute the search of JOHNSON's PHONES seized pursuant to this warrant as follows:

a. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachments A1 and B1 of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

b. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachments A1 and B1 to this Affidavit. In this particular case, the government anticipates the use of a "hash value" library to exclude normal operating system files that do not need to be searched, which would further facilitate the search for items described in Attachment B1. Further, the government anticipates the use of hash sets and known file filters to assist the digital forensics examiners/agents in identifying known and or suspected child

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

pornography image files. Use of these tools will allow for the identification of evidentiary files, but also assist in the filtering of normal system files that would have no bearing on the case.

c. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

d. Unless the government seeks an additional order of authorization from any Magistrate Judge in the District, the government will return any digital device that has been forensically copied, that is not an instrumentality of the crime, and that may be lawfully possessed by the person from whom it was seized, to the person from who it was seized within 90 days of seizure.

INSTRUMENTALITIES

53. Based on the information in this Affidavit, I also believe that JOHNSON's PHONES are instrumentalities of crime and constitute the means by which violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252(a)(2) (Receipt and Distribution of Child Pornography), and 2252(a)(4)(B) (Possession of Child Pornography) have been committed. Therefore, I believe that in addition to seizing the digital devices and phones to conduct a search of their contents as set forth herein, there is probable cause to seize those digital devices and phones as instrumentalities of criminal activity.

/////

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

54. Based on the foregoing, I believe there is probable cause that evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 2252(a)(2) (Receipt or Distribution of Child Pornography), and 2252(a)(4)(B) (Possession of Child Pornography) will be found on JOHNSON's PHONES, as more fully described in Attachment A1 to this Affidavit. I therefore request that the Court issue a warrant authorizing a search of JOHNSON's PHONES for the items more fully described in Attachment B1 to this Affidavit, incorporated herein by reference, and the seizure of any such items found therein.

JOHN WURSTER, Affiant
Special Agent
United States Secret Service

SUBSCRIBED AND SWORN before me this 29th day of October, 2014.

United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A1
PREVIOUSLY SEIZED PHONES TO BE SEARCHED

The below-listed items were taken from SHAWN DAVID JOHNSON pursuant to search warrants executed on 7/14/14 and 7/17/14 respectively. These items, collectively referred to as JOHNSON's PHONES, are presently located at the U.S. Secret Service Seattle Field Office Evidence Room:

a. One Samsung Galaxy S5 Cell Phone

b. One HTC First Cell Phone.

c. One Droid RAZR Cell Phone

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B1
SECTION 1
ITEMS TO BE SEARCHED FOR

The following records, documents, files, or materials that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography), 2252(a)(2) (Receipt or Distribution of Child Pornography), and 2252(a)(4)(B) (Possession of Child Pornography) which may be found on JOHNSON's PHONES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct in any format or media, including visual depictions purchased from the website "nudistwonderland.com";

2. Evidence of the use of the email addresses sdjdogg@gmail.com and sdjdogg@yahoo.com;

3. Email, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

7. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

8. Evidence of who used, owned or controlled JOHNSON's PHONES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

9. Evidence of malware that would allow others to control JOHNSON'S PHONES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of counter forensic programs (and associated data) that are designed to eliminate data from a digital device;

11. Evidence of times and dates JOHNSON's PHONES were used;

12. Any other electronically stored information (ESI) from JOHNSON's PHONES necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

SECTION 2
SEARCH TECHNIQUES

Searching the ESI for the items described in Section 1 of this Attachment B1 may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

In this particular case, the government anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched, which will facilitate the search for evidence that does come within the items described in Section 1 of Attachment B1. Further, the government anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and or suspected child pornography image files. Use of these tools will allow for the quick

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identification of evidentiary files but also assist in the filtering of normal system files that would have no bearing on the case.

Law enforcement personnel are authorized to execute the search of JOHNSON's PHONES, pursuant to this warrant, as follows:

a. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible, of JOHNSON's PHONES. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include the investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

b. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B1 to this Affidavit.

c. If, after conducting its examination, law enforcement personnel determine that either of JOHNSON's PHONES is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970